International Journal of Law
ISSN: 2455-2194, RJIF 5.12
www.lawjournals.org
Volume 3; Issue 1; January 2017; Page No. 51-58

Terrorism and Intelligence Failure in India: A Holistic Analysis

Dr. K V K Santhy
Assistant Professor, Department of Law, NALSAR University of Law, Hyderabad, Telangana, India

Abstract
Good intelligence will indeed be essential if fresh terrorist attacks are to be preempted and the terrorist organisations - not just al Qaeda but its off shoots and imitators - are to be destroyed on a long-term basis. At the same time, any intelligence agency within a democracy must adhere to other standards – democracies must live up to the high standards of their own liberal rhetoric uphold the ideas of democracy, liberty, and human rights universally rather than selectively and at a time when tightening up on security is necessary. Taking into account the growing threat of international terrorism, there are significant grounds for doubting whether legal safeguards and oversee and review mechanisms have kept pace with the developing methods and capacities of the intelligence community.

In some areas, there are laws and executive orders that apply, but these have been slow in coming and do not cover the wide range of moral issues our intelligence personnel encounter. In India, particularly, it is clear that we must do better. With our national security at stake, it is essential to have a serious non- partisan debate, find an acceptable middle ground, and give our spies the unambiguous guidelines they so urgently need.

The question that finally arises in the light of all of this is whether protecting the security of the state in the light of the terrorism threat should trump all other objectives and values within society. Its true that national security is a legitimate and primary concern of the state, particularly one like India which has been wracked by terrorism over the past decade – and yet we must remember that we essentially define ourselves by the importance we place on democratic value, human rights and civil liberties. Accordingly, we must strive to observe and uphold these values to the greatest extent possible: so while security is one value, it must compete with other values in society. The quest of intelligence control and oversee in the democratic state, then, is to enable agencies to produce effective security intelligence while ensuring that they operate within the law and in a way that is consistent with democratic norms and standards. This article analyzes the problem of terrorism and makes an effort to investigate the root causes of failure on all levels, including the legislative process and executive branch ineffectiveness, while also attempting to highlight best practices in European nations.

Keywords: Terrorism, terrorist attacks, United States, Rule of Law

Introduction

The new era of global terrorism was ushered in on the day 19 suicide bombers hijacked heavily fueled airliners and flew them into the World Trade Center and the Pentagon on the 11th of September, 2001. Much has happened since that fateful day, with India too mirroring 9/11 with 26/11; there is a general recognition that the global war on terror declared in response to the atrocities should now be seen as a long term struggle [1].

The war also has constantly changing contours – starting from 1984 when narco-terrorism was first recognized, state sponsorship of terrorism has been declining. With terrorist groups, therefore, increasingly needing new sources of funds, the drug business has stepped up to fill this need perfectly [2]. Terrorist organizations have thus become increasingly dependent on drug trafficking as one of several primary sources of revenue to fund terrorist activities [3]. The combination of the war on drugs and the war against terror has exacerbated an already grave situation and has necessitated a need for introspection. As foreign terrorist organizations become more heavily involved in the drug trade, hybrid organizations are emerging, foreign terrorist organizations that have morphed into one part terrorist organization, one part global drug cartel.

To take just one example, the Taliban is in essence, the face of twenty-first-century organized crime, a visage meaner and uglier than anything law enforcement or militaries have heretofore faced. These hybrids represent the most significant security challenge to governments worldwide [4].

The atrocities that have been committed by acts of terrorism worldwide highlight the importance of strong legal frameworks, of the international rule of law, and of the consequences of its disregard. Ultimately however, the impact of such attacks, be it on the domestic level or the international one, depends upon the responses to them and in turn on the reaction to those responses [5].

In this context, the role played by intelligence agencies becomes increasingly invaluable. Iintelligence involves understanding the motivations, thoughts, and plans of one's enemies. Multidisciplinary intelligence, including insights into the cultures and mindsets of terrorist organizations, is crucial to providing indications and warnings of possible attacks and is critical to illuminating key vulnerabilities that can be exploited and leveraged to prevent, preempt, and disrupt terrorist activities before they occur. Essentially, the first priority should always be to get there before the bomb goes off [6].

Developments in the intelligence policy and practice of numerous democratic states since the terrorist attacks of 9/11 have underscored the necessity of retaining their commitment to foundational democratic norms and core values whilst seeking to protect their societies from those who would destroy those norms and values. The attacks of 9/11 instigated an immediate drive among Western governments to implement measures to protect the public safety and national security of their states [7].

The findings by later enquiry committees namely, the Congressional Joint Inquiry into Intelligence Community

Activities [8], and by the National Commission on the Terrorist Attacks upon the United States [9] had troubling points to make about the state of intelligence in the United States. Both committees complained that the Central Intelligence Agency and the Federal Bureau of Investigation failed "to focus" as well as share relevant information and failed to assess the cumulative import of the intelligence gathered about a "probable terrorist attack." The two bodies, also cited "serious gaps" in the collection capabilities of the two organizations [10].

Good intelligence will indeed be essential if fresh terrorist attacks are to be preempted and the terrorist organizations - not just al Qaeda but its off shoots and imitators - are to be destroyed on a long-term basis [11]. At the same time, any intelligence agency within a democracy must adhere to other standards – democracies must live up to the high standards of their own liberal rhetoric uphold the ideas of democracy, liberty, and human rights universally rather than selectively and at a time when tightening up on security is necessary.

Taking into account the growing threat of international terrorism, there are significant grounds for doubting whether legal safeguards and oversee and review mechanisms have kept pace with the developing methods and capacities of the intelligence community.

Intelligence services the world over have thwarted many terrorist attacks since 2001, some of which have been publicized, others which have not. The scope of operations of intelligence agencies is broad and complex, and they deserve clearer guidelines. Unlike their military colleagues, they lack detailed rules of engagement, standing orders, and international conventions to define limits of behavior. In some areas, there are laws and executive orders that apply, but these have been slow in coming and do not cover the wide range of moral issues our intelligence personnel encounter. In India, particularly, it is clear that we must do better. With our national security at stake, it is essential to have a serious non- partisan debate, find an acceptable middle ground, and give our spies the unambiguous guidelines they so urgently need [12].

The question that finally arises in the light of all of this is whether protecting the security of the state in the light of the terrorism threat should trump all other objectives and values within society. Its true that national security is a legitimate and primary concern of the state, particularly one like India which has been wracked by terrorism over the past decade [13] – and yet we must remember that we essentially define ourselves by the importance we place on democratic value, human rights and civil liberties. Accordingly, we must strive to observe and uphold these values to the greatest extent possible: so while security is one value, it must compete with other values in society. The quest of intelligence control and oversee in the democratic state, then, is to enable agencies to produce effective security intelligence while ensuring that they operate within the law and in a way that is consistent with democratic norms and standards.

The need for introspection and regulatory body in India

1. Demarcating the Agencies

The Constitutional scheme at present has provided for the Union Government's power to enact legislation in this regard, with the Intelligence Bureau specifically finding mention in Entry 8 in the Union List [14]. There is a clear need for providing legislative oversee for these agencies, a need which can be articulated primarily on the grounds of efficiency and basic constitutional and administrative law.

The Intelligence Bureau, as mentioned earlier, functions is India's internal security agency. One of the longest functioning intelligence agencies, its roots can be traced back to the Imperial Intelligence Bureau, which served British interests in India [15]. It is chartered with a wide range of responsibilities spanning from combating terrorists and the separatist efforts of Naxalists to critical infrastructure protection – particularly aviation security [16]. The IB falls under India's Ministry of Home Affairs although the Director of the IB can report to the Prime Minister on intelligence issues [17].

On the other side, we have the Research and Analysis Wing of the Cabinet Secretariat. Until 1968, the IB also handled external intelligence. But after India's miserable performance in the 1962 border war with China, the need for a separate external intelligence agency was clear. As a result, India established its dedicated external intelligence agency, the Research and Analysis Wing. Founded mainly to focus on China and Pakistan, over the last forty years the organization has expanded its mandate and is credited with greatly increasing India's influence abroad [18].

It seems that not much is known regarding the structure of RAW. The organization started with 250 people and about $400,000. It has since expanded to several thousand personnel, but there is no clear estimate of its staffing or budget, as both remain secret. However, an estimate by the U.S.-based Federation of American Scientists suggests that in 2000, RAW had about eight to ten thousand agents and a budget that experts place at $145 million. Unlike the United States' Central Intelligence Agency or Britain's MI6, RAW reports directly to the prime minister instead of the Ministry of Defense. The chief of RAW is designated secretary (research) in the Cabinet Secretariat, which is part of the prime minister's office. Some officers of RAW are members of a specialized service, the Research and Analysis Service, but several officers also serve on deputation from other Services such as the Indian Police Service [19].

2. Reasons for Regulation beyond the terrorist threat

When looking at the recommendations of the Task Force headed by former RAW (Research and Analysis Wing) chief, Girish Chandra Saxena, an important point is made regarding giving the Intelligence Bureau complete responsibility for internal security operations [20] – for this it is clearly imperative that the IB have a formal charter. For a further delineation, it is important that the RAW should also have a written charter. Further, the concept of an "intelligence community" [21] that the recommendations talk about can only flourish when the internal organizations and tasking are based on professional management, with coordination requiring formal charters being established for each organization with minimal overlap

3. Concerns of Privacy

A major concern is that of Privacy. Following an expose by Outlook magazine of illegal phone tapping by the NTRO [22], it becomes imperative to look at the legal framework regarding the same:

First, we have Section 5 of the Indian Telegraph Act, which provides for the power for the Government to take possession of licensed telegraphs and to order interception of messages [23].

Over and above this was the Supreme Court judgment in the matter of *PUCL v. Union of India*, where a set of guidelines regarding telephone tapping where issued, as follows [24]:

1. An order for telephone-tapping in terms of Section 5(2) of the Act shall not be issued except by the Home Secretary, Government of India (Central Government) and Home Secretaries of the State Governments. In an urgent case the power may be delegated to an officer of the Home Department the Government of India and the State Governments not below the rank of Joint Secretary. Copy of the order shall be sent to the Review Committee concerned with one week of the passing of the order-.
2. The order shall require the person to whom it is addressed to intercept in the course of their transmission by means a public telecommunication system, such communications as are described in the order. The order may also require the person to whom it is addressed to disclose the intercepted material to such persons and in such manner as are described in the order.
3. The matters to be taken into account in considering whether an order is necessary under Section list of the Act shall include whether the information which is considered necessary to acquire could reasonably be acquired by other means.
4. The interception required under Section 5(2) of the Act shall be the interception of such communications as are sent to or from one or more addresses specified in the order belong an address or addresses likely to be used for the transmission of communications to or from, from one particular person specified or described in the order or one particular set of premises described in the order.
5. The order under Section 5(9) of the Act shall, unless renewed, case to have effect at the end of the period of two month from the date of issue. The authority which issued the order may, at any time before the end of two month period renew the order if it by the State Government. (a) The Committee shall on its own, within two months of the passing of the order by the authority concerned, investigate whether there is or has been a relevant order under Section 5(2) of the Act. Where there is or has been an order whether there has been any contravention of the provisions of Section 5(2) of the Act. (b) If on an investigation the Committee concludes that there has been a contravention of the provisions of Section 5(2) of the Act, it shall set aside the order under scrutiny of the Committee. It shall further direct the destruction of the copies of the intercepted material. (c) If on investigation, the Committee comes to the conclusion that there has been no contravention of the provisions of Section considers that it is necessary to continue the order in terms of Section 5(2) of the Act. The total period for the operation of the order shall not exceed six months.
6. The authority which issued the order shall maintain the following records:

a. The intercepted communications
b. The extent to which the material is disclosed
c. The number of persons and their identity to whom any of the material is disclosed
d. The extent to which the material is copied and
e. The number of copies made of any of the material.

7. The use of the intercepted material shall be limited to the minimum that is necessary in terms of Section 5(2) of the Act.
8. Each copy made of any of the intercepted material shall be destroyed as soon as its retention is no longer necessary in terms of Section 5(2) of the Act.
9. There shall be a Review Committee consisting of Cabinet Secretary, the Law Secretary and the Secretary, Telecommunication at the level of the Central Government. The Review Committee at the State level shall consist of Chief Secretary, Law Secretary and another member, other than the Home Secretary, appointed 5(2) of the Act, it shall record the finding to that effect.

Thus it is clear from reading the above that only specific phone numbers may be intercepted, which are to be detected by the intelligence authority prior to the interception, with accompanying justification, the number being required before the process of interception begins. Following submission of the number to the Home Secretary, it requires confirmation and written authorization before the interception of the number can begin.

While we thus have an acknowledgement of the fact that the government is required to resort to some degree of intelligence-gathering aided by the growth of highly sophisticated communication technology for purposes of national security, it is also true, as the Outlook expose has shown, that the prevalent safeguards have not been very effective. The following extract from the expose, quoting a member of the NTRO is illuminative [25]:

> *"As we said, if you don't have a specific phone number, then how can you authorise its interception? If the target is a VIP, why will the Union home secretary give a written authorisation? One also has to note that this equipment is sent out to keep searching for that one possible number among thousands which may be of value from a national security point of view. By then, however, you have already intercepted a thousand calls and all of them illegally. The vehicles are deployed every day in some part of the country or the other, mostly in Delhi. On no single occasion did the vehicle go out with the authorisation of the home secretary. We did try to safeguard a few VIPs, including senior intelligence officials, by creating a set of mobile numbers, which could not be tapped. If the machine detected this number while scanning, it would shut down immediately. But how many private, top secret numbers can we secure and protect in the long run? If Sonia Gandhi or Rahul Gandhi's numbers are not on that list, we can tap them as well. That is the system's greatest strength and weakness."*

4. The Perils of Politicization

Politicization is another major peril, that has resulted from lack of oversee mechanisms. As is indicated in the wire-tapping cases, it is unfortunate that a chunk of the agencies' focus has been on political surveillance and election-related information gathering in support of the ruling party [26]. As one member of the National Security Advisory Board commented recently, "How can we expect the IB to function if a large part of its resources is directed at serving the ruling political party of the day?" [27] It is imperative for a

clear distinction to be drawn between security of the state, and security of the government [28].

Questions of efficiency come to the fore when we consider issues of unclear strategic guidance and obscured responsibilities that plague the functioning of the agencies presently. Considering further that assessments made by intelligence agencies act as the point of departure for law enforcement units to act, it is important that the substratum of information be strong and reliable.

Current processes, whether they be of internal operations or oversee, are clearly lacking: RAW maintains no permanent distinction between covert operatives who execute secret tasks, and personnel who must liaise with services such as the CIA or public bodies, such as analysts and area specialists. As a result, personnel with sensitive operational information are exposed to potentially compromising contacts [29]. Further, there has been seen to be a large amount of resistance within the RAW to its in-house surveillance group, termed the Counter-Intelligence Security Division. In 1980, RAW personnel actually went on strike against the CIS Division's surveillance, claiming it was unnecessary harassment. A Delhi police officer attached to the CIS Division was held hostage in his room while RAW staffers took out a protest procession [30].

Considering, finally, that intelligence is a tool required by a country's policy makers and planners to further her global and regional interests, it is important that broader policy concerns certainly have the people's representatives conducting a review of the same.

Proposal for an Ideal Framework of Accountability

1. Broad levels of Accountability

We may at the onset identify three types of accountability: horizontal, vertical, and the 'third dimension' [31]. Horizontal accountability is the term used to describe the restraint of state institutions by other state institutions, public agencies and the three branches of government (executive, legislative and judiciary). It is considered horizontal because it implies a relationship among co-equals, that is, among independent state agencies.

In contrast, 'vertical accountability' concerns relations among those unequal in their power relations, such as the hierarchical relationship between senior officials (principals) and their subordinates (agents) within a state institution. This can also be referred to as 'control'. Vertical accountability also applies to the efforts of citizens, the media and civil society organisations to keep public officials acting in accordance with good standards. Citizens, civil society groups and other non-state actors are considered part of vertical accountability mechanisms because they have much less power relative to state actors to influence the target institutions because of the state's control over the means of coercion, resources and means of communication. The vertical accountability process may be top–down, as in the case of principals controlling agents in a bureaucracy, or bottom–up, as in the case of citizens holding their elected representatives accountable at election time.

The third type of accountability relationship is the 'third dimension'. This refers to the role of international actors, such as foreign governments, intergovernmental organisations and international non-governmental organisations in holding a state institutional actor to account. It could be argued that the European Court of Human Rights, for example, increasingly constitutes a 'third dimension' accountability mechanism for security and intelligence services of EU member states [32].

2. The Four-tier Framework

From a democratic governance point of view, the oversee of the intelligence services is a shared responsibility of the executive, the legislature and the judiciary. A sound system of checks and balances is necessary, in which the executive does not have the exclusive privilege of overseeing the intelligence services. Thus, the intelligence agencies themselves, national parliaments, as well as external review bodies all have a role to play in this end eavour. If we were to demarcate the exact levels at which oversee would need to be developed, they would be:

1. Internal control at the level of the agency
2. Executive control
3. Parliamentary oversee
4. Oversee by independent oversee bodies

The standards and mechanisms that will be discussed in the following chapters will take reliance on the "best practices" that the Report sanctioned by the Geneva Centre for the Democratic Control of Armed Forces, the Norwegian Parliamentary Intelligence Oversee Committee and the Human Rights Centre of the University of Durham titled "Making Intelligence Accountable: Legal Standards and Best Practices for Oversee" makes, along with taking a comparative approach and looking at legislation in different countries to establish the best possible framework for India. This chapter will enumerate in brief the recommendations that the Report makes at the four tiers.

Starting with the first tier, looking at the level of internal control, it will start with clear definition of the role and sphere of the agency in the establishing legislation, taking into account the exceptional powers granted to them, as well as the need for delineating their functions, so that their special powers are not used in routine situations where there is no preeminent threat to the state [33].

The exercise of special powers granted to intelligence agencies needs to be scrutinized, taking into account the importance of grounding such powers in the rule of law, proportionality, and controls against misuse when they encroach on civil liberties [34]. There may be controls before the exercise of the power, such as the authorization of an external person, or controls after the exercise, such as laws governing what information can be retained, and how it can be used, and for what purposes [35]. Holding of personal data also requires to be governed by certain standards.

The next tier is in the instance of executive oversee: effective parliamentary oversee depends on effective control of the agencies by the ministers. Important here is to make a clear demarcation between the respective functions of ministers and agency heads [36]. Next off, the importance of an open door policy towards the agency by the Minister should be kept in mind. Control over Covert Action is another aspect that must be looked into. Safeguards against ministerial abuse must also be made: First, looking at the potential abuse that can take place, such as using information gathered for the purpose of domestic politics, various safeguards are put to keep a check on executive oversee, such as writing down of ministerial instructions,

disclosing them to another agency, and the ministerial requirement to brief the Leader of the Opposition [37].

Next comes the case for Parliamentary oversee. It is essential for ensuring that the agencies are serving the state as a whole and not narrower political/sectional interests, giving legitimacy and democratic accountability [38].

Looking into the Mandate of Parliamentary Oversee bodies, there are 2 ways of defining it: Firstly, the horizontal scope of the mandate that would be the entire intelligence community, including all ancillary departments and officials, should be covered by the mandate of one or more parliamentary oversee bodies; Secondly, the vertical scope of the mandate of a parliamentary oversee body might include some or all of the following (a) legality, (b) efficacy, (c) efficiency, (d) budgeting and accounting; (e) conformity with relevant human rights Conventions (f) policy/administrative aspects of the intelligence services [39].

3. Parliamentary Regulatory Body

The Composition of a Parliamentary Oversee Body should represent a cross-section of political parties, and ensure a clear demarcation between the body and the agencies being regulated themselves. Appointment of members of the body is another issue that requires consideration [40]. Vetting of members should be carried out in cases where the committee's mandate deals with operationally sensitive material, with the criteria for vetting being defined clearly [41].

The need for the oversee body to have sufficient access to relevant information and documents from the intelligence agencies, and thus the legal power to initiate investigations, is another important issue. Consultation of external expertise would come under this ambit, thus allowing the Parliament to receive alternate viewpoints. This should be accompanied by clear prohibitions with respect to unauthorized disclosure of such documents. Taking budget control to be at the heart of Parliamentary control, there must be a transparent process of budget-making. Intelligence Agencies should only use funds for the purpose for which they were authorized by the Legislative branch.

Finally, the role of external review bodies would be significant: taking into account that redressal of grievances through the normal court system in the case of intelligence agencies would be somewhat ineffective seeing the problems that would arise with production of evidence amongst other matters, there must be an alternate system of redressal [42].

4. Composition of the Body

The Composition of a Parliamentary Oversee Body should represent a cross-section of political parties, and ensure a clear demarcation between the body and the agencies being regulated themselves [43]. In that sense, while relevant experience is an important consideration, so is the fact that the members be civilian. Co-optation can otherwise be a problem, i.e., the situation where members and staff come to identify more with the intelligence agencies than with their roles as detached and objective supervisors: a complaint seen, for instance, in the case of the U.S. Congressional Oversee Committees, where a section have been members of the agencies formerly [44].

Appointment of members of the body is another issue that requires consideration. There are different levels of involvement by executive across the board in different countries: the UK has maximum executive involvement, with the head of government appointing. The provision of appointment is as follows:

> *The Committee shall consist of nine members (a) who shall be drawn both from members of the House of Commons and from members of the House of Lords and (b) none of whom shall be a Minister of the Crown;*
> *The members of the Committee shall be appointed by the Prime Minister after consultation with the Leader of the Opposition* [45].

The other end of the spectrum is in the case of Norway, where it is the legislature which is solely concerned with the appointment process:

> *The Committee shall have seven members including the chairman and vice-chairman, all elected by the Storting, on the recommendation of Presidium of the Storting, for a period of a maximum of five years. Steps should be taken to avoid replacing more than four members at the same time* [46].

A balanced take is found in the Australian legislation: here, the role of nomination and appointment is divided between the executive and the legislature respectively, with the Prime Minister being required to consult the leaders of all other Parliamentary parties before making nominations [47].

A number of countries have vetting procedures for the Committee members; however, such security clearances would only be required if the Committee were to be dealing with so-called "operationally sensitive" material [48]: something that is attempted to be kept out of the ambit.

The need for the oversee body to have sufficient access to relevant information and documents from the intelligence agencies, and thus the legal power to initiate investigations, is another important issue. Consultation of external expertise would come under this ambit, thus allowing the Parliament to receive alternate viewpoints. This should be accompanied by clear prohibitions with respect to unauthorized disclosure of such documents.

5. Further Considerations

There must also be a legal duty on the oversee body to report back at least annually. Tied into this idea is the extent to which certain information can be reported publicly: it may be remembered for instance, that the Joint Task Force led by Girish Saxena resulted in a report that had large sections deleted on account of being sensitive. It is important to maintain a balance here: thus, while it should be open to the agencies to make representations regarding certain material in the report that may be considered sensitive, it should be the Parliamentary Committee which has the final word. To maintain the idea of Parliamentary "ownership" of the Committee, it would be recommended that the Committee report directly to Parliament rather than through the Government [49].

Taking budget control to be at the heart of Parliamentary control [50], there must be a transparent process of budget-making. Intelligence Agencies should only use funds for the purpose for which they were authorized by the Legislative branch.

Executive Regulation

Effective Parliamentary oversee would go hand in hand with, and in fact depend on effective executive oversee. Parliaments can only reliably call ministers to account for the actions of the intelligence agencies if ministers have real powers of control and adequate information about the actions taken in their name. The nature of governmental structure makes them better equipped to direct and manage matters at a closer level [51].

1. Demarcating Responsibility

At the onset, it must be emphasized that effective control by the executive must be distinguished from direct managerial responsibility: a clear line must be drawn between the agencies and the ministers.

In the UK, the chief of the respective intelligence service has to make an annual report on the work of the service to the Prime Minister and the Secretary of State. The Secretary of State further authorizes special powers of the agency such as entry or interference with property or with wireless telegraphy [52].

Further reference may be made to the Canadian Security Intelligence Service Act, 1984, which refers to the Director of the Service having 'the control and management of the Service' that is 'under the direction' of the Minister.

Again, the Polish Internal Security Agency and Foreign Intelligence Agency Act, 2002 makes a clear distinction, where Article 7 puts forth that the Prime Minister shall define the directions of the Agencies' activities by means of instructions, while the Heads of the Agencies are to periodically present the Prime Minister with plans of action.

2. Checks against Executive Abuse

Experience demonstrates considerable misuse of the intelligence service apparatus for motivations personal and political, with the aforementioned NTRO expose possibly the tip of the iceberg. As the experience of Report of the Joint Task Force headed by Girish Saxena [53] goes, there is the risk of excessive secrecy where the government may attempt to withhold information about security accountability or procedures which are legitimate matters of public debate, under the guise of "national security". Safeguards here must work on two levels: first to protect against abuse taking place, and second, to protect those who highlight such abuse or refuse to obey orders which may be seen as illegal. For this second aspect, reference may be made to the whistle-blowing provisions mentioned earlier.

The first basic safeguard would be to ensure that executive directions are put in writing: a number of legislations across the board feature this requirement. The Canadian Security Intelligence Service Act, for instance, after stating that the Director of the agency concerned has control and management of the Service *under* the direction of the Minister, provides for the Minister to issue written directions with respect to the service. The statute further provides for a copy of such directions to be forwarded to the Review Committee [54].

To maintain a bipartisan approach, it would be relevant to look at the provision in Australian law, whereby the Director-General is necessarily required to brief the leader of Opposition, thereby ensuring that opposition Parliamentarians do not feel that they have been excluded from the "ring of secrecy" [55].

Finally, an explicit declaration that the agency does not take any action to further the interests of any political party may be put in as an overarching safeguard to prevent political abuse, as has been done in UK legislation [56]. The UK may also be noted for providing for an open-door policy of access to the Prime Minister by the agency heads [57].

External review body

Security and intelligence agencies are often trusted with exceptional powers, such as surveillance or security clearance, which, if used incorrectly or mistakenly, carry the risk of serious injustice to individuals. It is therefore important that some avenue of redress should be open to people who suspect that they may have been the victim of an injustice, for example those whose private life may have been intruded upon or whose career may have been affected. Moreover, in a security or intelligence agency, as with any large body, complaints can highlight administrative failings and lessons to be learned, leading to improved performance [58].

However, precisely because of the secret nature of the processes involved, difficulties in obtaining evidence, and the legitimate need of these agencies to protect sensitive information from public disclosure, redress through public hearings in the regular courts is rarely effective or appropriate. There is also the need to ensure that any system for redress cannot be used by the legitimate targets of a security or intelligence agency to find out about the agency's work. Achieving a balance in any complaints system between independence, robustness and fairness, on the one hand, and sensitivity to security needs on the other is challenging but not impossible. We can thus look at judicial processes on the one hand, and non-judicial processes on the other.

1. Judicial Procedures

The courts and judiciaries have a direct impact on the protection of rights of individuals and on the exercise of democratic control over state institutions, in particular executive branch institutions. As intelligence and security are realms dominated by executive action, creating accountable intelligence and internal security structures relies especially on judicial review of the legality of government actions, the degree of judicial activism as revealed by willingness of the courts to strike down laws and actions deemed to be unlawful or unconstitutional. In such ways, the judiciary helps to hold government bodies responsible for the use and possible misuse of power. Creating effective, independent and impartial judiciaries is a crucial factor in the development and enforcement of rule of law and therefore of democratisation.

More specifically, the judicial branch is also an important component of creating a security intelligence apparatus that is effective yet limited in its powers, that operates within the rule of law, is accountable, and is subject to democratic and civilian control. In a democracy, the judiciary plays an important role in upholding the law, enforcing the constitution and democratic rights and procedures, and adjudicating disputes that cannot or should not be decided by the executive or legislative branches or private individuals. The judiciary also plays a monitoring role in ensuring that the other branches of government act within the law. Through judicial or constitutional review, the judiciary can prevent the arbitrary exercise of power by the

government. In the case of internal security, independent judicial review is essential for the resolution of conflicts between national security claims and the principles of human rights and civil liberties.

2. Other external review mechanisms

In some cases, the Parliamentary Oversee Committee may deal with complaints, as is the case in Germany and Norway [59]. The problem with this would be lack of independence. A specialist tribunal may be established to deal with complaints either against a particular agency or in relation to the use of specific powers, as in the United Kingdom. To combat the task of access of evidence in this special situation, special security-cleared counsel have been introduced in Canada and the U.K., who have the task of challenging security –related arguments. Further, Independent Auditing agencies are required to certify that the expenditure of the agencies is in compliance with the law in an independent and effective manner.

Conclusion

The global war on terror will be long and deadly. It will be the defining reality of this generation and quite possibly beyond. The importance of combating terrorism at its source has to be understood by addressing the scourges of poverty, discrimination, and disenfranchisement. The challenges and opportunities for diplomacy – domestic and international - and aid may never have been greater.

This paper has endeavoured to, at one level, highlight the importance of intelligence oversee in such a framework, and at the second level, examine the different levels on which such an oversee structure would be effective. In India, there is an absence of an established process of appointment for both potential officers and the head of the agency. It is imperative that legislation must establish the process of appointment, including minimum qualifications. Such processes must be subject to scrutiny by Parliament or at least the leader of the opposition. Further, like other positions of authority and responsibility-tenure and criterion for removal must be clearly specified by law. This not only assures quality of candidates, but also acts as insulation from pressure by the government, and places a premium on merit rather than connections and pliability.

While the legal framework is obviously important due to its role in establishing the official mandate of a security intelligence agency and its relationships with other key institutions, the legislature and judiciary, it is not necessarily the only approach to understanding control of internal security structures in democratic states. Of greater and more fundamental importance are basic political values such as respect for dissenting ideas, human rights and privacy; acceptance and legitimacy of a system of effective public oversee; a concept of national security that is limited to core political values and societal interests; and strict requirements for justifying the holding back of information from parliament and the public and restricting the rights and freedoms of citizens.

In tandem with legislation, it is the internalization of these political values and ideas within the political culture, especially among the political elite, that provides the most essential indicator of democratic governance of the security sphere. In essence, these go a long in way strengthening the base of democracy and the rule of law, which in turn would aid in combating the scourge of terrorism.

References

1. Steve Tsang (ed.), Intelligence and Human Rights in the Era of Global Terrorism, 2007, p. 1.
2. Gen. James L. Jones, U.S. Nat'l Sec. Advisor, Speech at the 45th Munich Security Conference (Feb. 8, 2009), as mentioned in John E. Thomas Jr., *Narco-Terrorism: Could the Legislative and Prosecutorial Responses threaten our Civil Liberties?* 66 Wash. & Lee L. Rev. 2009.
3. Chris J. Nolan, *United States' Narcoterrorism Policy: A Contingency Approach on the Convergence of the Wars on Drugs and against Terrorism*, 4 Review of Policy Research (22) 2005.
4. Michael Braun, Drug Trafficking and Middle Eastern Terrorist Groups: A Growing Nexus?, in Countering Transnational Threats: Terrorism, Narco-Trafficking and WMD Proliferation (Matthew Levitt & Michael Jacobson) eds., 2009), as available in Chris J. Nolan, *United States' Narcoterrorism Policy: A Contingency Approach on the Convergence of the Wars on Drugs and against Terrorism*, 4 Review of Policy Research (22) 2005.
5. Helen Duffy, The War on Terror and the Framework of International Law, p. 1.
6. Frank Cilluffo and Ronal Marks, *The Use and Limits of U.S. Intelligence*, 1 The Washington Quarterly (25) 2002.
7. Hans Born and Marina Caparini, Democratic Control of Intelligence Services: Controlling Rogue Elephants, 2007, p. 10.
8. Congressional Joint Inquiry into Intelligence Community Activities, available at http://www.gpoaccess.gov/serialset/creports/911.html, last accessed 30-09-2010.
9. National Commission on the Terrorist Attacks upon the United States, available at http://www.9-11commission.gov, last accessed 30-09-2010.
10. Jeffery Richelson, *The Quest for Absolute Security: The Failed Relations among U.S. Intelligence Agencies*, 4 Journal of Cold War Studies (11) 2009.
11. Steve Tsang (ed.), Intelligence and Human Rights in the Era of Global Terrorism, Praeger Security International, 2007.
12. James Olson, *Intelligence and the War on Terror: How Dirty Are We Willing to Get Our Hands?*, 1 SAIS Review (28) 2008.
13. Other than the aforementioned 26/11 attack on Mumbai, notable incidents of terrorism have occurred over the past decade in Delhi, Bangalore, Pune, Jaipur, and other attacks in Mumbai.
14. Entry 8, List I, Schedule 7, Constitution of India.
15. *The Intelligence Bureau: India's Prime Intelligence Agency*, available at http://frontierindia.net/the-intelligence-bureau-india's-prime-intelligence-agency, last accessed 15-10-2010.
16. Ministry of Home Affairs, Annual Report 2006-07 (Government of India: 2007), 28, 31-32; http://mha.nic.in/Annual-Reports/ar0607_Eng.pdf, last accessed 15-10-2010.
17. Ibid.

18. Jayshree Bajoria, *RAW: India's External Intelligence Agency*, available at http://www.cfr.org/publication/17707/raw.html, last accessed 10-10-2010.
19. Ibid.
20. Bhashyam Kasturi, *The Intelligence Secret*, available at =: http://www.ipcs.org/article/military/the-intelligence-secret-589.html, last accessed 12-10-2010.
21. Praveen Swami, *Stalled Reforms*, available at: http://www.hinduonnet.com/fline/fl2009/stories/20030509002108700.htm, last accessed 12-10-2010.
22. Saikat Datta, *Bootleg Tapes: The Rulers Who Listen; "Give Us Legal Immunity, We'd Be Happy To Provide Proof Of Illegal Tapping"*, available at www.outlookindia.com/article.aspx?265272, www.outlookindia.com/article.aspx?265273, *last accessed 02-10-2010.*
23. *(1) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do, take temporary possession (for so long as the public emergency exists or the interest of the public safety requires the taking of such action) of any telegraph established, maintained or worked by any person licensed under this Act.*
    (2) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order:
    *Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section*The Indian Telegraph Act, No. 13 of 1885.
24. *People's Union for Civil Liberties v. Union of India and Ors.*, 1997 (1) SCC 318.
25. Saikat Datta, *Bootleg Tapes: The Rulers Who Listen; "Give Us Legal Immunity, We'd Be Happy To Provide Proof Of Illegal Tapping"*, available at www.outlookindia.com/article.aspx?265272, *www.outlookindia.com/article.aspx?265273.*
26. Ibid.
27. Saikat Datta, *War Below the Radar*, New Delhi Outlook, 31 July 2006, p.1; http://www.outlookindia.com, last accessed 10-10-2010.
28. Vikram Sood, *Intelligence Reform*, http://soodvikram.blogspot.com/2007/06/intelligence-reform-or-perish.html, last accessed 09-10-2010.
29. Praveen Swami, *Half-Baked Reforms at RAW*, available at http://www.hindu.com/2006/07/05/stories/2006070505341100.htm.
30. Praveen Swami, *How the Mole Watchers were shackled*, available at http://www.hindu.com/2004/06/15/stories/2004061505751100.htm, last accessed 05-10-2010.
31. Derek Brinkerhoff, *Taking Account of Accountability: A Conceptual Overview and Strategic Options*, Centre for Democracy and Governance, as available at www.usaid.gov/our_work/democracy_and_governance/publications/ipc/wp-14.pdf, last accessed 15-10-2010.
32. Ibid at p. 17.
33. Ibid at p. 29.
34. Ibid at p. 37.
35. Ibid at p. 46.
36. Ibid at p. 55.
37. Ibid at p. 68.
38. Ibid at p. 77.
39. Ibid at p. 80.
40. Ibid at p. 85.
41. Ibid at p. 88.
42. Ibid at p. 105.
43. Born and Leigh, Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies, p. 85.
44. Loch K. Johnson, *Governing in the absence of Angels: On the Practice of Intelligence Accountability in the United State*s, 57 in Born, Johnson and Leigh, Who's Watching the Spies: Establishing Intelligence Service Accountability, 61.
45. Section 10, Intelligence Services Act, 1994.
46. Section 1, Instructions for Monitoring of Intelligence, Surveillance and Security Services, 1995.
47. Section 14, Intelligence Services Act, 2001.
48. Born and Leigh, Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies, p. 89.
49. Ibid at 94.
50. Ibid at 96.
51. Born and Leigh, Page 55.
52. Section 5, Intelligence Services Act, 1994.
53. Bhashyam Kasturi, *The Intelligence Secret*, available at: http://www.ipcs.org/article/military/the-intelligence-secret-589.html.
54. Section 6, Security Intelligence Service Act, 1984.
55. Born at 69.
56. Section 2, Security Service Act, 1989; Section 2 and Section 4, Intelligence Services Act, 1994.
57. Section 2, Intelligence Services Act, 1994.
58. Born and Leigh, Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies, p. 105.
59. F. Sejersted, *Intelligence Oversight in Norway*, available at www.dcaf.ch/legal_wg/ev_oslo_030919_sejersted.pdf, last accessed 16-10-2010.